SVERIGE

(19) SE

(12) **PATENTSKRIFT** (13) **C2** (11) **517 116**

(51) Internationell klass [7]
H04L 9/32

PATENT- OCH REGISTRERINGSVERKET

(45) Patent meddelat **2002-04-16**
(41) Ansökan allmänt tillgänglig **2002-02-12**
(22) Patentansökan inkom **2000-08-11**
(24) Löpdag **2000-08-11**
(62) Stamansökans nummer
(86) Internationell ingivningsdag
(86) Ingivningsdag för ansökan om europeisk patent
(83) Deposition av mikroorganism

(30) Prioritetsuppgifter

(21) Patentansöknings-nummer **0002962-9**

Ansökan inkommen som:

[X] svensk patentansökan
[ ] fullföljd internationell patentansökan med nummer
[ ] omvandlad europeisk patentansökan med nummer

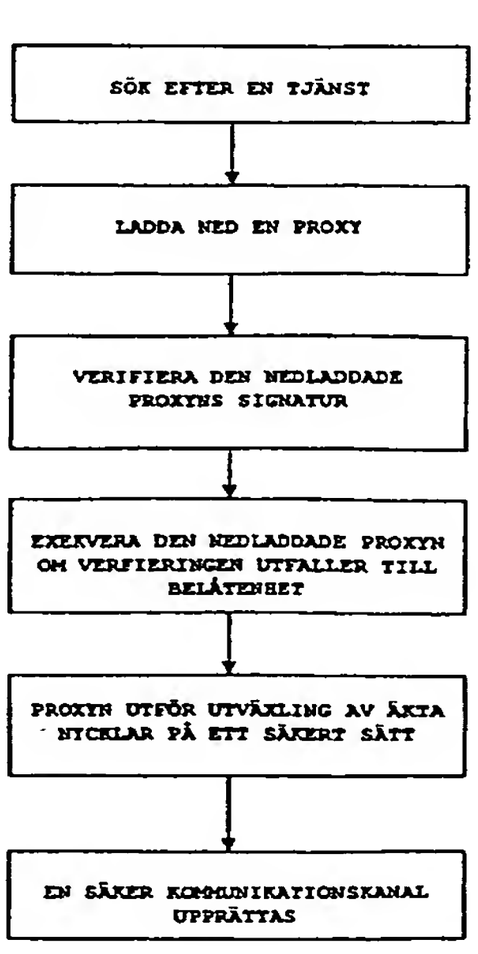
(73) PATENTHAVARE Telefonaktiebolaget L M Ericsson, 126 25 Stockholm SE
(72) UPPFINNARE Christian Gehrmann, Stockholm SE
(74) OMBUD Ericsson Radio Systems AB

(54) BENÄMNING Metod och anordning för säkra kommunikationstjänster

(56) ANFÖRDA PUBLIKATIONER: - - -

(57) SAMMANDRAG:

Föreliggande uppfinning rör säkrandet av information i öppna system och mer specifikt en metod och ett system för säkerställandet av äkthet och integritet samt skyddandet av konfidentiell information i samband med nyttjandet av godtyckliga kommunikationstjänster. En klient som önskar kommunicera med en specifik tjänst laddar ned en signerad programkod från denna tjänst, vilken programkod innehåller nödvändig kod för utväxling och verifiering av äkta nycklar med nämnda tjänst. Det antas att klienten endast stödjer två stycken grundläggande krypteringsfunktioner, nämligen signering av godtyckligt data medelst användandet av en offentlig-nyckel-algoritm tillsammans med en envägs hashfunktion samt förmåga att verifiera godtyckligt datas signatur. Antalet nödvändiga i förväg definierade säkerhetsfunktioner som en klient eller server måste stödja begränsas genom nedladdning av det för nyckelutväxlingen och kommunikationssäkerheten nödvändiga protokollet. Detta innebär dessutom att det blir betydligt enklare att uppdatera kommunikationssäkerheten eftersom endast servrarnas programvara behöver uppdateras.



PRV Patent använder följande dokumentkoder för sina patentskrifter

kod	klartext
A	allmänt tillgänglig patentansökan
B	utläggningsskrift *
B5	rättad utläggningsskrift *
C	patentskrift *
C1	patentskrift *
C2	patentskrift
C3	rättad patentskrift
C5	rättad patentskrift *
C8	korrigerad förstasida till patentskrift
F	patentskrift i ändrad lydelse
F8	korrigerad förstasida till patentskrift i ändrad lydelse
F9	rättad patentskrift i ändrad lydelse

kod	klartext
L	allmänt tillgänglig
T1	översättning av kraven i europeisk patentansökan
T2	rättelse av översättning av kraven i europeisk patentansökan
T3	översättning av europeisk patentskrift
T4	översättning av europeisk patentskrift i ändrad avfattning
T5	rättad översättning av europeisk patentskrift
T8	rättad översättning av europeisk patentskrift
T9	korrigerad översättning av europeisk patentskrift

* publicerad under äldre lagstiftning

Nationskoder

AP	African Regional Industrial Property Organization (ARIPO)
EA	Euroasian Patent Office (EAPO)
EP	Europeiska Patentverket (EPO)
OA	African Intellectual Property Organization (OAPI)
WO	World Intellectual Property Organization (WIPO)
IB	WIPO (i vissa fall)
AD	Andorra
AE	Förenade Arabemiraten
AF	Afghanistan
AG	Antigua
AI	Anguilla
AL	Albanien
AM	Armenien
AN	Nederländska Antillerna
AO	Angola
AR	Argentina
AT	Österrike
AU	Australien
AZ	Azerbajdzjan
BA	Bosnien och Hercegovina
BB	Barbados
BD	Bangladesh
BE	Belgien
BF	Burkina Faso
BG	Bulgarien
BH	Bahrain
BI	Burundi
BJ	Benin
BM	Bermuda
BO	Bolivia
BR	Brasilien
BS	Bahamaöarna
BT	Bhutan
BW	Botswana
BY	Vitryssland
BZ	Belize
CA	Kanada
CF	Centralafrikanska Republiken
CG	Kongo
CH	Schweiz
CI	Elfenbenskusten
CL	Chile
CM	Kamerun
CN	Kina
CO	Colombia
CR	Costa Rica
CU	Kuba
CV	Kap Verde
CY	Cypern
CZ	Tjeckiska republiken
DE	Tyskland
DJ	Djibouti
DK	Danmark
DM	Dominica
DO	Dominikanska republiken
DZ	Algeriet
EC	Ecuador
EE	Estland
EG	Egypten
ES	Spanien
ET	Etiopien
FI	Finland
FJ	Fiji-öarna
FK	Falklandsöarna
FR	Frankrike
GA	Gabon
GB	Storbritannien
GD	Grenada
GE	Georgien
GH	Ghana
GI	Gibraltar
GM	Gambia
GN	Guinea
GQ	Ekvatorial Guinea
GR	Grekland
GT	Guatemala
GW	Guinea-Bissau
GY	Guyana
HK	Hongkong
HN	Honduras
HR	Kroatien
HT	Haiti
HU	Ungern
ID	Indonesien
IE	Irland
IL	Israel
IN	Indien
IQ	Irak
IR	Iran
IS	Island
IT	Italien
JM	Jamaica
JO	Jordanien
JP	Japan
KE	Kenya
KG	Kirgistan
KH	Kambodja
KI	Kiribati
KM	Comorerna
KN	St Kitts
KP	Dem. Folkrepubliken Korea
KR	Republiken Korea
KW	Kuwait
KY	Cayman-öarna
KZ	Kazachstan
LA	Laos
LB	Libanon
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Litauen
LU	Luxembourg
LV	Lettland
LY	Libyen
MA	Marocko
MC	Monaco
MD	Moldavien
MG	Madagaskar
MK	Makedonien
ML	Mali
MM	Mayanmar
MN	Mongoliet
MR	Mauretanien
MS	Monsterrat
MT	Malta
MU	Mauritius
MV	Maldiverna
MW	Malawi
MX	Mexiko
MY	Malaysia
MZ	Mocambique
NA	Namibia
NG	Nigeria
NI	Nicaragua
NL	Nederländerna
NO	Norge
NP	Nepal
NR	Nauru
NZ	Nya Zeeland
OM	Oman
PA	Panama
PE	Peru
PG	Papua Nya Guinea
PH	Filippinerna
PK	Pakistan
PL	Polen
PT	Portugal
PY	Paraguay
RO	Rumänien
RU	Ryska Federationen
RW	Ruanda
SA	Saudi-Arabien
SB	Salomonöarna
SC	Seychellerna
SD	Sudan
SE	Sverige
SG	Singapore
SH	St Helena
SI	Slovenien
SK	Slovakien
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia
SR	Surinam
ST	São Thomé
SV	El Salvador
SY	Syrien
SZ	Swaziland
TD	Tchad
TG	Togo
TH	Thailand
TJ	Tadzjikistan
TM	Turkmenistan
TN	Tunisien
TO	Tonga
TR	Turkiet
TT	Trinidad och Tobago
TV	Tuvalu
TW	Taiwan
TZ	Tanzania
UA	Ukraina
UG	Uganda
US	Förenta Staterna (USA)
UY	Uruguay
UZ	Uzbekistan
VA	Vatikanstaten
VC	St Vincent
VE	Venezuela
VG	Jungfruöarna
VN	Viet Nam
VU	Vanuatu
WS	Samoa
YD	Syd-Jemen
YE	Jemen
YU	Yugoslavien
ZA	Sydafrika
ZM	Zambia
ZR	Zaire
ZW	Zimbabwe

TEKNISKT OMRÅDE

Föreliggande uppfinning rör allmänt sett säkrandet och skyddandet av information i öppna kommunikationssystem och mer specifikt en metod och ett system som tillhandahåller integritetsskydd, skyddar konfidentiell information samt kontrollerar och fastställer äktheten avseende viss information, under användandet av godtyckliga kommunikationstjänster.

TEKNIKENS STÅNDPUNKT

I öppna kommunikationssystem finns ett behov av att säkra och skydda informationen. Detta omfattar kontroll och säkerställandet av deltagande parters äkthet, att integritetsskydda utväxlad information och att säkerställa att informationen förblir konfidentiell under kommunikationen. Säkerställandet av äkthet innebär att medel används för att garantera att parterna verkligen är de de utger sig för att vara, eller att utsänd/skickad information ej på något sätt har manipulerats av icke behörig/a. Säkerställandet av att informationen förblir konfidentiell innebär att ingen obehörig kan avlyssna, läsa eller på något sätt ta del av våra data. Integritetsskydd innebär säkerställandet av att meddelandet ej ändrats, d.v.s. att meddelandet är i ursprungligt skick och ej manipulerats eller ändrats på något sätt och att hela meddelandeströmmen kommer från en och samma avsändare och mottas av en och samma mottagare.

Lösningar på dessa typer av problem kommer från forskningen inom krypteringsområdet. En krypteringsalgoritm är typiskt sett en funktion som har ett värde som skall hållas hemligt eller som skall skyddas vid inmatning samt ett annat hemligt värde

som används vid inmatning. Det hemliga värdet kallas ofta för en för algoritmen hemlig nyckel. Många moderna säkra kommunikationssystem använder välkända krypteringsalgoritmer och säkerheten baseras inte på algoritmen i sig utan på en hemlig nyckel. Antagandet att endast den faktiska nyckeln hemlighålls från illasinnade kallas Kerkhoff:s antagande. Kerkhoff:s antagande är viktigt i öppna kommunikationssystem som Internet, i vilka anordningar från olika leverantörer och tillverkare skall kunna fungera tillsammans på många skilda platser. Det är betydligt enklare att få kommunikationen att fungera om databearbetningsmetoderna är allmänt kända. Således bygger samtliga på Internet förekommande tekniker för säker kommunikation på Kerkhoff:s antagande, det vill säga allmänt kända krypteringsalgoritmer i vilka säkerheten baseras på hemliga nycklar eller hemliga värden för nycklar.

För att en säker kommunikationskanal skall kunna upprättas måste det finnas någon form av i förväg definierat protokoll som beskriver vilka meddelanden som skall utväxlas mellan parterna som deltar i kommunikationen. Ett nödvändigt steg för att säkra ett kommunikationssystem är att tillhandahålla utväxling och verifiering av äkta nycklar. Typiskt sett sker utväxlandet av nycklar medelst en offentlig-nyckel-algoritm, det vill säga en algoritm som använder sig av ett nyckelpar bestående av en offentlig och en privat nyckel, övers. anmn., till exempel Diffie-Hellman-algoritmen, vilken till exempel används i Internets protokoll vid utväxling av nycklar IKE, (Internet Key Exchange Protocol), transportlagrets säkerhetsprotokoll TLS, (Transport Layer Security protocol) och det "säkra skalprotokollet" SSH, (Secure Shell Protocol), eller RSA-algoritmen (Rivest-Shamir-Adleman) som till exempel används i TLS.

I öppna säkerhetsprotokoll såsom SSH, TLS och IPsec/IKE (Internet Protocol Security), används offentlig-nyckel-algoritmer för digital signering eller för att utväxla nycklar.

Ett flertal olika metoder för signering medelst offentliga-privata-nyckelpar såväl som metoder för att utväxla nycklar kan användas. Det grundläggande protokollet som används för att kryptera användardata samt lägga till en extra sträng för integritetskontroll sker på ett likartat sätt i protokollen. Dock skiljer sig protokollen avsevärt vad gäller procedurerna för att verifiera äkthet, att utväxla nycklar, samt stöd för de olika symmetriska algoritmerna. Ett problem är således att åtminstone en part i kommunikationen måste ha stöd för ett väldigt stort antal olika krypteringsalgoritmer och säkerhetsval om två enheter utan en redan i förväg definierad säkerhetsrelation skall kunna fungera tillsammans på ett säkert sätt. Dessutom gör det stora antalet valmöjligheter förhandlingsprotokollen för nycklarna mycket stora och komplicerade och de blir därför svåra att realisera.

Dokumentet US 5,892,904 beskriver en metod som säkerställer äkthet och integritet för ett dataprogram, en exekverbar fil, eller kod, erhållen från ett datanätverk, till exempel Internet. I en utföringsform omfattar metoden fastställandet av en kryptografisk summakod eller "hashvärde" som utgivaren använder för att signera nämnda dataprogram, exekverbara fil eller kod. Utgivarens signatur skapas med hjälp av en signeringsalgoritm vilken använder sig av offentliga-privata-nyckelpar, till exempel RSA-algoritmen (Rivest-Shamir-Adleman). Ett digitalt certifikat bifogas utgivarens signatur vilket bevisar utgivarens äkta identitet. Det digitala certifikatet innehåller uppgifter om programvaruutgivarens namn, en offentlig nyckel som matchar utgivarens privata nyckel vilken används för att signera nämnda programvara, fil eller kod, ett utgångsdatum för certifikatets giltighet och en länk eller hyperlänk till organisationen som utfärdat certifikatet.

Dokumentet WO 99/56428 beskriver en annan säker metod för att ladda ner ett program till en processor från en extern anordning. Programmet kan vara krypterat och ha tillagd

information för att styrka äkthet. Processorn dekrypterar och kontrollerar äktheten innan programmet tillåts exekveras av processorn.

Dokumentet WO 99/33224 beskriver en metod och ett system vilka säkerställer att en dataström som till exempel innehåller ljud- och bilddata endast kan mottas av behöriga. Mottagarna kan även bevisa antalet mottagna bild- och ljuddatapaket. Detta sker genom att varje datapaket som sänds krypteras och genom att logga antalet dekrypterade datapaket i mottagaren.

Inget av dessa dokument beskriver hur en säker kommunikationskanal upprättas mellan två parter som inte har en redan i förväg definierad säkerhetsrelation. Detta är en vanlig situation, till exempel i specifika för ändamålet upprättade nätverk, så kallade ad-hoc-nätverk, det vill säga Bluetooth™, Salutation™, Jini™ etc.. Det föreligger således ett behov av att få fram en metod och system vilka kan upprätta en säker kommunikation mellan en klient och en godtycklig kommunikationstjänst.

SAMMANFATTNING AV UPPFINNINGEN

Föreliggande uppfinning tillhandahåller en lösning på problemet att säkra en kommunikationskanal mellan två parter vilka inte har en redan i förväg definierad säkerhetsrelation.

I protokoll enligt teknikens ståndpunkt måste åtminstone en av parterna stödja ett mycket stort antal olika krypteringsalgoritmer och valmöjligheter avseende säkerhet om två enheter skall kunna fungera tillsammans, vilket gör förhandlingsprotokollen avseende krypteringsnycklarna stora och komplicerade.

En målsättning med föreliggande uppfinning är således att tillhandahålla en lösning där antalet nödvändiga i förväg definierade krypteringsalgoritmer är så få som möjligt.

En annan målsättning med föreliggande uppfinning är att göra förhandlingsprotokollen avseende krypteringsnycklarna mindre komplicerade, vilket beror av antalet nödvändiga valmöjligheter för säkerhet och antalet nödvändiga krypteringsalgoritmer.

Ytterligare en målsättning med föreliggande uppfinning är att tillhandahålla en lösning där problemet med exportrestriktioner (av data) kan minskas.

Ovan nämnda målsättningar uppnås fundamentalt genom att klienten laddar ned en signerad datorprogramkod (till exempel en Jini™-Proxy) från den specifika kommunikationstjänst som klienten önskar kommunicera med, vilken programkod innehåller de nödvändiga algoritmerna för utväxling och verifiering av äkta nycklar med servern. Dessutom innehåller datorprogrammet de nödvändiga algoritmerna för att kryptera och skydda allt data som utväxlas under en säker tjänstesession.

Mer specifikt rör uppfinningen en situation då en klient vill kommunicera med en speciell tjänst på ett säkert sätt. Tjänsten kan nås via ett globalt nätverk såsom Internet, ett lokalt nätverk eller rent av via ett ad-hoc-nätverk, det vill säga ett för ändamålet skapat nätverk "i flykten" av enheter som råkar befinna sig på samma plats. Det antas även att samtliga enheter som använder sig av tjänsten använder en gemensam plattform, d.v.s. att alla enheter kan ladda ner och exekvera ett program skrivet i ett gemensamt programspråk. Ett exempel på en vitt spridd och använd sådan plattform och programspråk är den virtuella Java™-maskinen och programspråket Java™. Klienten antas ha endast två i förväg definierade krypteringsförmågor; förmågan att signera godtyckligt data och förmågan att verifiera signerat godtyckligt data.

Servern som önskar tillhandahålla en säker kommunikationstjänst signerar (digitalt) ett datorprogram som innehåller de nödvändiga algoritmerna för utväxling och verifiering av äkta nycklar med servern medelst sin privata nyckel, vilken nyckel ingår i nyckelparet bestående av en offentlig och en privat

nyckel. Servern packar den signerade koden tillsammans med signaturen och eventuellt även ett eller flera certifikat vilka intygar äktheten av serverns offentliga nyckel. Serverns offentliga nyckel kan sedan användas för att verifiera kod som signerats av servern.

En klient som önskar kommunicera med en tjänst laddar ner paketet med den signerade koden och eventuellt även ett certifikat och kontrollerar paketets signatur. Om klienten har tillgång till en tillförlitlig offentlig nyckel som matchar signaturen eller om klienten hyser tillit för någon av de offentliga nycklarna som ingår i de bifogade certifikaten så behandlar klienten den nedladdade koden som en pålitlig säkerhetskod.

Säkerhetskoden exekveras sedan på den gemensamma plattformen av klienten och kan uppmana klienten att utföra en säkerhetsfunktion om ömsesidig identitetskontroll önskas. Denna funktion har godtyckligt data som indata och som utdata en digital signatur för indatat plus en av klienten tillagd specifik etikett. Klienten kan också returnera ett certifikat som innehåller en offentlig nyckel som tjänsten kan använda för att verifiera signaturer utförda av klienten. Tjänstekoden utför utväxling och verifiering av äkta nycklar med sin ursprungliga server. Om detta lyckas upprättar den vidare en säker kommunikationslänk med servern.

I en första utföringsform av föreliggande uppfinning sker utväxling och verifiering av äkta nycklar på ett mer effektivt sätt genom utnyttjandet av det faktum att själva koden för nyckelutväxlingen i sig är signerad, och därmed undviks skapandet av en signatur för en offentlig nyckel samt en verifiering av nämnda signatur samt en dataöverföring mellan klienten och servern.

I en andra utföringsform av föreliggande uppfinning separeras utväxlandet av nycklar från skyddandet av kommunikationen. Fördelen med detta angreppssätt är att ett flertal olika

tjänster kan skyddas genom användandet av en huvudnyckel i stället för att varje tjänst måste utföra ett tungt utväxlande av offentliga nycklar.

Genom att tillåta nedladdning av kod avseende säkerhetsprotokoll för utväxling av nycklar samt datakommunikation begränsas antalet i förväg definierade säkerhetsfunktioner som en server eller klient måste stödja. Säkerheten garanteras istället genom signering av själva säkerhetskoden. Detta innebär även att det blir betydligt enklare att uppdatera säkerhetsskyddet för kommunikationen med nya algoritmer, eftersom endast serverns programvara behöver uppdateras då eventuella säkerhetsbrister upptäcks och hela, eller delar av, programvaran måste skrivas om.

Eftersom klientens nödvändiga krypteringsfunktioner endast omfattar signering och verifiering av signaturer uppträder normalt sett inga problem med exportrestriktioner eftersom dessa funktioner normalt sett ej är försedda med exportrestriktioner.

KORT RITNINGSBESKRIVNING

Dessa uppfinningens målsättningar och fördelar blir mer uppenbara och tydliga genom följande detaljerade beskrivning med tillhörande figurer, vilka har referensnummer för motsvarande delar, och där:

Figur 1 visar det grundläggande kommunikationsscenariot;

Figur 2 visar ett flödesdiagram för en utföringsform av uppfinningen

Figur 3 illustrerar ett alternativt kommunikationsscenario med användande av en server för nyckelutväxling.

BESKRIVNING AV FÖREDRAGNA UTFÖRINGSFORMER

Föreliggande uppfinning skall nu beskrivas, med hänvisning till figur 1, i en situation 100 som kräver säker kommunikation i vilken en kommunicerande klient 110 önskar kommunicera med en server 120 som tillhandahåller vissa speciella tjänster. Servern 120 kan nås av klienten 110 via ett globalt nätverk, t.ex. Internet, eller ett lokalt nätverk eller rent av via ett ad-hoc-nätverk 130. Det förutsätts vidare att samtliga enheter som använder tjänsten använder en gemensam plattform för databearbetning 140, d.v.s. samtliga enheter kan ladda hem och exekvera ett dataprogram skrivet i ett gemensamt programspråk. Ett exempel på en sådan vitt spridd och använd plattform för databearbetning och programspråk är Java™:s virtuella maskin och programspråket Java™. Enheten vilken tillhandahåller tjänsten, d.v.s. servern 120, har fullständig kännedom om programspråket och den gemensamma plattformen för databearbetningen som de olika klienterna 110 i nätverket använder.

Uppfinningen skall nu beskrivas med användandet av Java™-Jini™-teknik som ett exempel på en klient som önskar ansluta sig till en kommunikationstjänst. Java™-Jini™-tekniken gör det möjligt för datorer och anordningar att snabbt upprätta ad-hoc-nätverk utan planering, installation eller mänskligt ingripande. Varje anordning tillhandahåller tjänster som andra anordningar i nätverket kan använda sig av. Dessa anordningar har även egna gränssnitt, vilket säkerställer hög tillförlitlighet och kompatibilitet. Varje anordning och tjänst finns registrerad i en uppslagstjänst, och då nya anordningar inträder i nätverket går de igenom ett ”inträdesprotokoll” (add-in protocol) benämnt ”hitta och anslut” (discovery and join). För att använda en tjänst söker en person eller ett program upp tjänsten med användande av uppslagstjänsten. Tjänstens gränssnitt kopieras från uppslagstjänsten till anordningen som framställt tjänsteförfrågan, i vilken anordning gränssnittet kommer

användas. Uppslagstjänsten agerar således som en kopplingsstation i det den ansluter en klient sökande efter en specifik tjänst med denna tjänst. Det spelar ingen roll var tjänsten finns realiserad eftersom kompatibiliteten är säkerställd genom att varje tjänst tillhandahåller alla nödvändiga attribut för samverkan med nämnda tjänst medelst en nedladdningsbar Jini™ proxy.

Tillit är ett centralt problem i trådlösa ad-hoc-nätverk. Eftersom vi inte kan lita på mediet är vårt enda val att använda oss av kryptering. Ett av huvudproblemen är att vi inte kan förutsätta att några i förväg definierade säkerhetsrelationer finns mellan noderna i ad-hoc-nätverket. Givet att samtliga noder i ad-hoc-nätverket har offentliga-privata nyckelpar, och att samtliga noder hyser tillit till övriga noders offentliga nycklar för att upprätta säkra anslutningar inom ad-hoc-nätverket, kan en godtycklig identitets/äkthetskontroll baserad på offentliga-privata nyckelpar användas.

Till skillnad från olika standarders angreppssätt förutsätter inte föreliggande uppfinning att både klienten och servern nödvändigtvis stödjer en stor uppsättning olika algoritmer för symmetrisk nyckelkryptering och kryptografiska kontrollsummor, så kallade "MAC"-koder (Message Authentication Code). Det förutsätts i stället att klienten endast har två stycken i förväg definierade krypteringsförmågor:

- Klienten kan digitalt signera godtyckligt data medelst en offentlig-nyckel-algoritm samt en envägs hashfunktion; och

- Klienten kan verifiera riktigheten av godtyckligt data som signerats medelst en offentlig-nyckel-algoritm. Algoritmerna som används för signering av data utväljs från ett mycket litet antal möjliga algoritmer.

Mjuk- och/eller hårdvaran som används för att signera godtyckligt data samt för att verifiera signerat godtyckligt data, är fysiskt placerad i klienten och realiserad på ett sätt vilket gör den omöjlig att ändra eller manipulera för icke behöriga. Mjuk- och/eller hårdvaran som används för signering eller för att verifiera signaturer behöver inte endast använda den gemensamma plattformen, t.ex. kan "API"-gränssnitt (Application Program Interfaces) definierade i plattformen användas i stället.

Genom att använda de ovan beskrivna krypteringsförmågorna, kan en klient ladda ned en "Jini™-proxy" på ett säkert sätt, och använda nämnda Jini™-proxy för att exekvera ett protokoll rörande säkerställandet av äkthet och nyckelhantering på egen hand. Detta ger total frihet att använda tjänstespecifika säkerhetslösningar. Nu skall en första utföringsform av uppfinningen beskrivas med hänvisning till flödesschemat i figur 2.

Före det att någon kommunikation äger rum förbereder servern en Jini™-proxy som klienten kan ladda ner. Servern signerar även nämnda Jini™-proxy och möjliggör på så sätt för klienten att verifiera nämnda Jini™-proxys integritet och ursprung före det att nämnda Jini™-proxy exekveras. Nämnda Jini™-proxys kod inkluderar typiskt sett en offentlig nyckel vilken motsvaras (matchas) av en privat nyckel på servern samt nödvändiga metoder för utväxling och verifiering av äkta nycklar med servern.

1. En server som önskar erbjuda säker kommunikation har ett datorprogram, skrivet i ett programspråk som ingår i den gemensamma plattformen, d.v.s. Java. Med Jini™-terminologi säger vi att servern har en Jini™-proxy. Jini™-proxyn innehåller de nödvändiga algoritmerna samt metoderna för

utväxling och verifiering av äkta nycklar med servern. Dessutom innehåller nämnda proxy de nödvändiga krypteringsalgoritmerna för säker kommunikation mellan en klient och en server under en säker tjänstesession. Proxyn behöver dock inte nödvändigtvis innehålla all nödvändig kod för de kryptografiska beräkningarna. Istället kan proxyn använda API-gränssnitt definierade i den gemensamma plattformen, om detta är möjligt.

2. Servern signerar digitalt Jini™-proxyn med användande av sin privata nyckel. Signaturen beräknas med hjälp av de ovan beskrivna i förväg definierade algoritmerna och formaten. Detta säkerställer att klienten kan kontrollera signaturens äkthet.

3. Servern packar den signerade koden tillsammans med signaturen och möjligtvis även ett eller flera certifikat vilka certifierar serverns offentliga nyckel. Serverns offentliga nyckel kan användas för att styrka serverns äkthet.

I Jini™, och liknande miljöer, initieras kommunikationen av en klient som söker en tjänst. Då väl tjänsten hittats, laddar klienten ned tjänstens proxy för exekvering, med den skillnaden att nämnda proxys äkthet verifieras före det att proxyn exekveras.

4. En klient söker efter en tjänst med användande av Jini:s uppslagstjänst 200.

5. Då klienten hittar tjänsten och önskar använda sig av nämnda tjänst, laddar klienten ned en proxy som motsvarar nämnda tjänst tillsammans med signaturer och möjligtvis även certifikat 210.

6. Klienten verifierar att det nedladdade datapaketets signatur är äkta. Om klienten har en pålitlig offentlig nyckel som motsvarar (matchar) signaturen, alternativt om klienten litar på någon av de bifogade certifikatens offentliga nycklar, så behandlar klienten den nedladdade koden som pålitlig kod 220.

7. Om verifieringen av proxyn utfaller till belåtenhet, exekverar klienten den nedladdade koden medelst den gemensamma plattformen. Lämpliga restriktioner för när och hur exekveringen skall ske kan läggas till, specifikt behöver den nedladdade koden inte kunna kommunicera med någon annan server än den angivna servern 230.

Den nedladdade koden kan be klienten skapa en signerad biljett om ömsesidigt styrkande av äkthet krävs. Klienten kan vägra utföra några andra kryptografiska funktioner. Biljetten skapas genom att något godtyckligt data signeras och att en speciell etikett läggs till av klienten. Etiketten behövs för att säkerställa att det resulterande datat alltid känns igen som en biljett. Klienten kan även returnera ett certifikat innehållande en offentlig nyckel som kan användas till att styrka äktheten av klientens signatur. Biljettens etikett anger typiskt vilken tjänst klienten bett proxyn om samt en tidsstämpel. Etiketten skall visas för klientens användare före datat och etiketten signeras. Användaren kan i det läget vägra signera biljetten. I så fall kan Jini™-proxyn och servern verifiera varandras äkthet på följande sätt:

8. Proxyn utför utväxling och verifiering av äkta nycklar med sin ursprungliga server 240. Protokollet som används för det säkra utväxlandet av äkta nycklar kan i grunden vara något standardprotokoll för verifiering av äkthet och nyckelutväxling, t.ex. DH eller RSA. Jini™-proxyn kan begära ett certifikat från klienten vilket intygar den offentliga nyckelns äkthet, vilken nyckel används för att verifiera

biljettens signatur enligt ovan. Om äktheten är bevisad, upprättar proxyn en säker kommunikationslänk med servern 250.

Tjänsteleverantören som skriver säkerhetskoden kan realisera algoritmen för utväxlandet av nycklar enligt eget gottfinnande, men skall följa goda vedertagna principer för kryptering. Säkerhetsnivån beror således av hur serverns algoritm är utformad.

I en första utföringsform av uppfinningen utnyttjas det faktum att koden för utväxlandet av nycklar i sig är signerad av servern så att serverns offentliga nyckel ej behöver signeras. På så sätt sparas bearbetningsresurser genom att skapandet av en signatur undviks samt även kommunikationsresurser genom att koden för nyckelns signatur ej behöver överföras från servern till klienten. Dessutom sparas ytterligare bearbetningsresurser eftersom klienten ej behöver verifiera den offentliga nyckelns signatur. Detta förfarande är möjligt eftersom signaturen för programkoden, vilken styr utväxlandet av nycklar, verifieras före själva utväxlandet av nycklar. Således har klienten redan tillgång till information för att avgöra huruvida serverns nyckel är äkta. Till exempel, om Diffie-Hellman används, kan värdet tillhörande serverns offentliga nyckel finnas i koden som styr tjänsten. Således kan nyckelutväxlingen utföras genom endast en överföring från klienten till servern och vi sparar en överföring.

I en andra utföringsform enligt föreliggande uppfinning, vilken illustreras i figur 3, separeras utväxlandet av nycklar från själva kommunikationsskyddet. Fördelen med detta angreppssätt är att ett flertal olika tjänster kan skyddas med en för en grupp tillhörande huvudnyckel, i stället för att varje tjänst skall behöva utföra en resurskrävande utväxling av offentliga nycklar. I stället för att söka efter en tjänst söker klienten 300 således efter en server för nyckelutväxling 310. Klienten 300 erhåller en huvudnyckel gällande en viss grupp samt en

identifierare för denna huvudnyckel från servern 310. Då sedan klienten 300 önskar använda sig av en tjänst belägen i samma domän i vilken servern för nyckelytväxlingen befann sig, söker klienten efter en server 320 som tillhandahåller en tjänst, laddar ned ett paket från servern 320 och exekverar paketet på den gemensamma plattformen 330. Den nedladdade säkerhetskoden kan begära att klienten 300 utför en säkerhetsfunktion, vilken har huvudnyckelns identifierare som indata och huvudnyckeln som utdata, där nämnda huvudnyckel gäller en viss grupp. Vid utväxlandet av nycklar använder den nedladdade koden som styr tjänsten nämnda huvudnyckel.

Uppfinningen har nu beskrivits med användande av Jini™-teknologi i rent illustrativt syfte för att ge ett exempel på hur uppfinningen kan realiseras. Uppfinningen kan dock realiseras på en rad andra sätt, det enda kravet är att noderna stödjer en gemensam plattform, det vill säga att samtliga noder i ad-hoc-nätverket kan ladda ned och exekvera programkod skriven ett gemensamt programspråk samt förmågan att skapa och verifiera signaturer. Uppfinningen kan till exempel även användas vid upprättandet av säkra WAP- (Wireless application protocol) tjänster, det vill säga genom att ladda ned ett program som definierar säkerhetsalgoritmen.

Ovan beskrivna utföringsformer tjänar endast ett illustrativt syfte och skall ej ses som begränsningar. Det är uppenbart för en fackman att avvikelser kan göras från ovan beskrivna utföringsformer utan att avvika från uppfinningens omfång och andemening. Uppfinningens omfång skall ej betraktas såsom begränsat till de beskrivna exemplen utan skall istället betraktas såsom likvärdigt med följande patentkrav.

PATENTKRAV

1. En metod för att upprätta en säker kommunikationskanal mellan en klient och en server, i vilken nämnda klient och server har en gemensam plattform som stödjer digital signering av godtyckligt data och verifiering av nämnda godtyckliga datas signatur, nämnda metod **kännetecknad av,**

att klienten laddar hem ett digitalt signerat datapaket från servern vilket datapaket innehåller procedurer för att utföra utväxling och verifiering av äkta nycklar med servern,

att klienten verifierar nämnda datapakets digitala signatur, samt,

att nämnda datapaket exekveras på nämnda gemensamma plattform om nämnda verifiering utfaller till belåtenhet.

2. Metoden enligt kravet 1 vidare **kännetecknad av** att nämnda nedladdade datapaket uppmanar klienten att utföra en säkerhetsfunktion med godtyckligt indata och en digital signatur för nämnda godtyckliga data som utdata samt en av klienten tillagd etikett för ömsesidig verifikation avseende äkthet.

3. Metoden enligt kravet 2 **kännetecknad av att** nämnda etikett är tidsstämplad samt består av en text som identifierar den efterfrågade tjänsten.

4. Metoden enligt något av föregående krav **kännetecknad av** att nämnda gemensamma plattform för databearbetning är Java:s virtuella maskin samt programspråket Java.

5. Metoden enligt något av föregående krav **kännetecknad av** att nämnda server är en server för utväxling av nycklar vilken tillhandahåller en huvudnyckel gällande en viss grupp

vilken huvudnyckel säkrar kommunikationen för ett flertal olika tjänster.

6. Ett system för upprättandet av en säker kommunikationskanal mellan en klient och en server, i vilket nämnda klient och server har en gemensam plattform för databearbetning vilken stödjer digital signering av godtyckligt data och verifiering av nämnda godtyckliga datas signatur,

nämnda system **kännetecknat av,**

organ för att ladda ned ett digitalt signerat datapaket från servern till klienten, vilket datapaket innehåller procedurer för utväxling och verifiering av äkta nycklar med servern,

organ nödvändiga för att klienten skall kunna verifiera det nedladdade datapaketets signatur, samt,

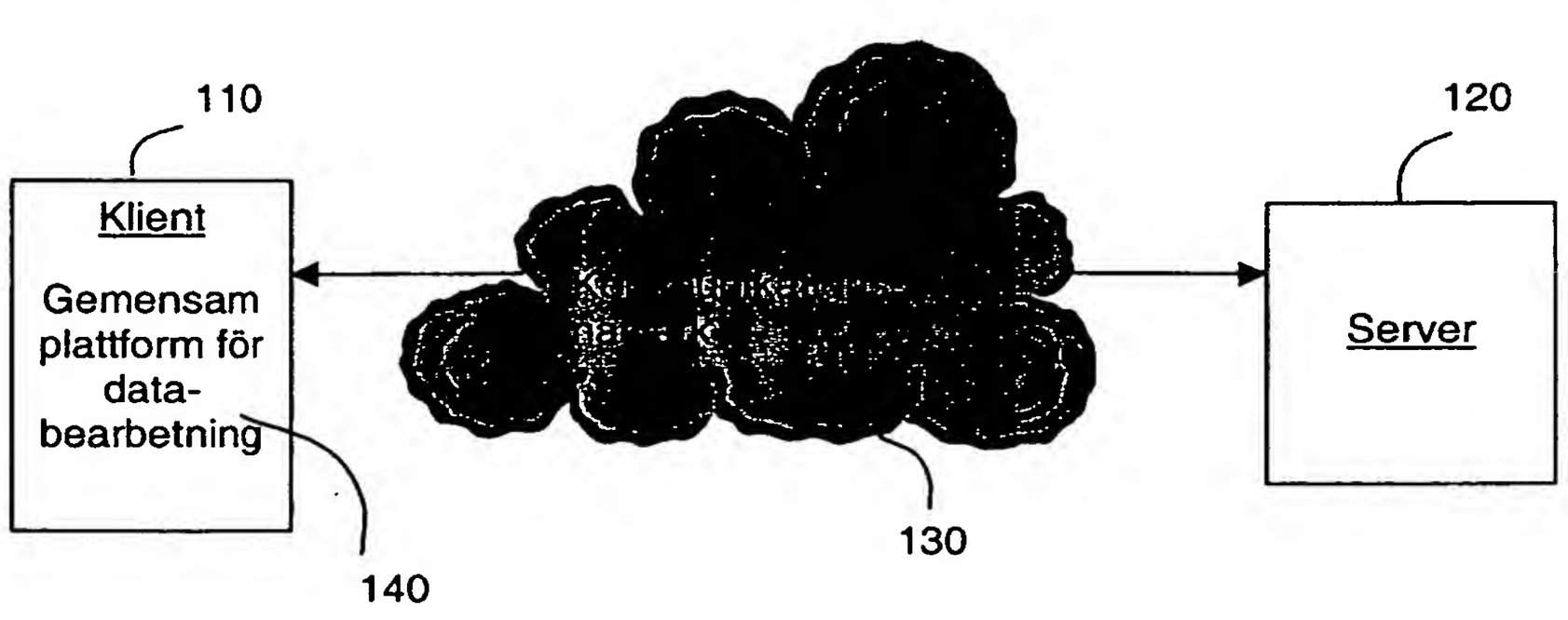
organ för att exekvera nämnda datapaket på nämnda gemensamma plattform för databearbetning i händelse nämnda verifiering utfaller till belåtenhet.

7. Systemet enligt kravet 6 vidare **kännetecknat av** att nämnda nedladdade datapaket innehåller instruktioner för att uppmana klienten att utföra en säkerhetsfunktion med något godtyckligt data som indata och en digital signatur för nämnda godtyckliga data som utdata samt en av klienten tillagd etikett för ömsesidig verifiering av äkthet.

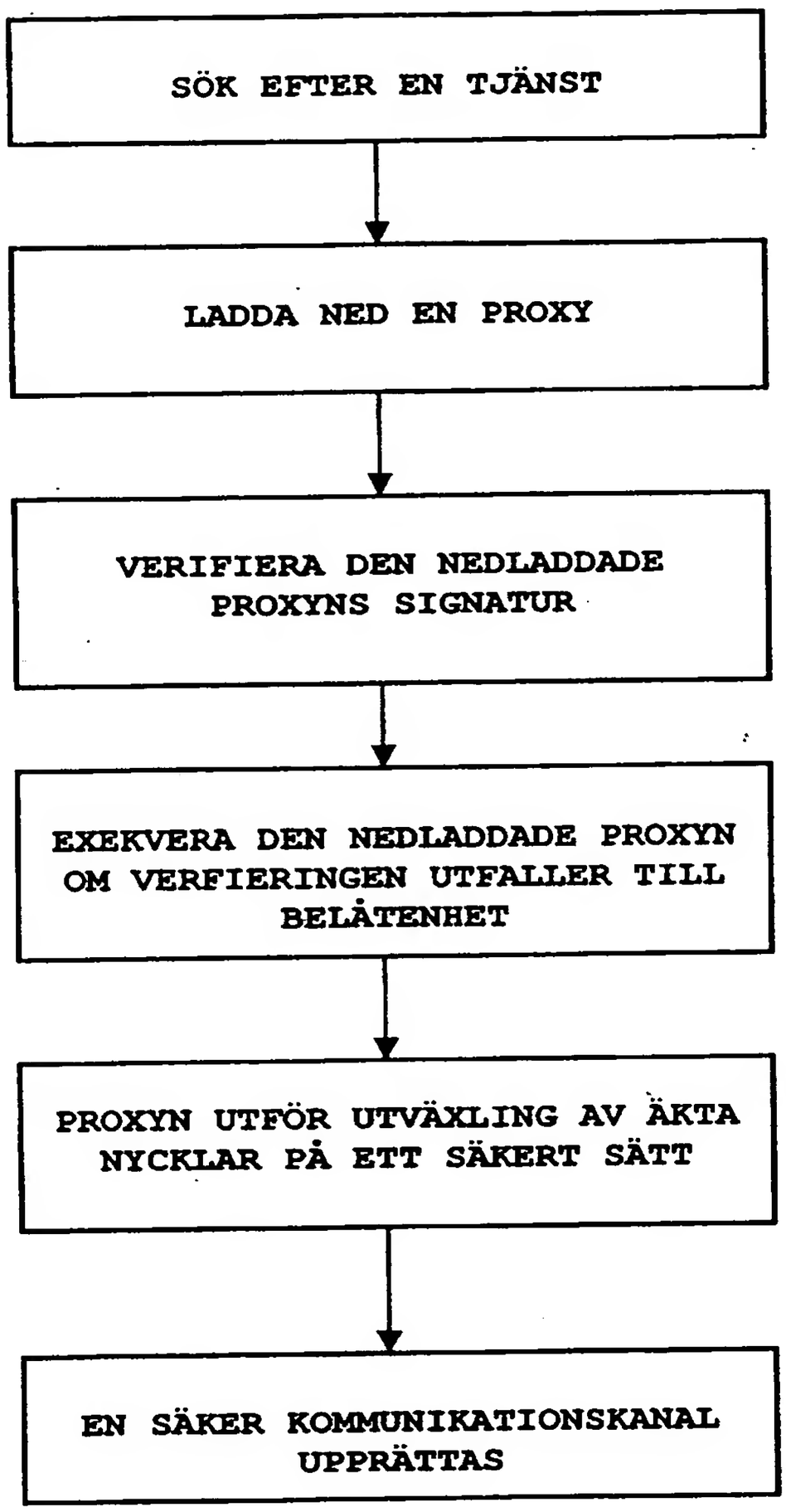
8. Systemet enligt kravet 8 **kännetecknat av** att nämnda etikett är en med en tidsstämpel försedd text som identifierar den efterfrågade tjänsten.

9. Systemet enligt något av kraven 6-8 **kännetecknat av** att nämnda gemensamma plattform för databearbetning är Java:s virtuella maskin och programspråket Java

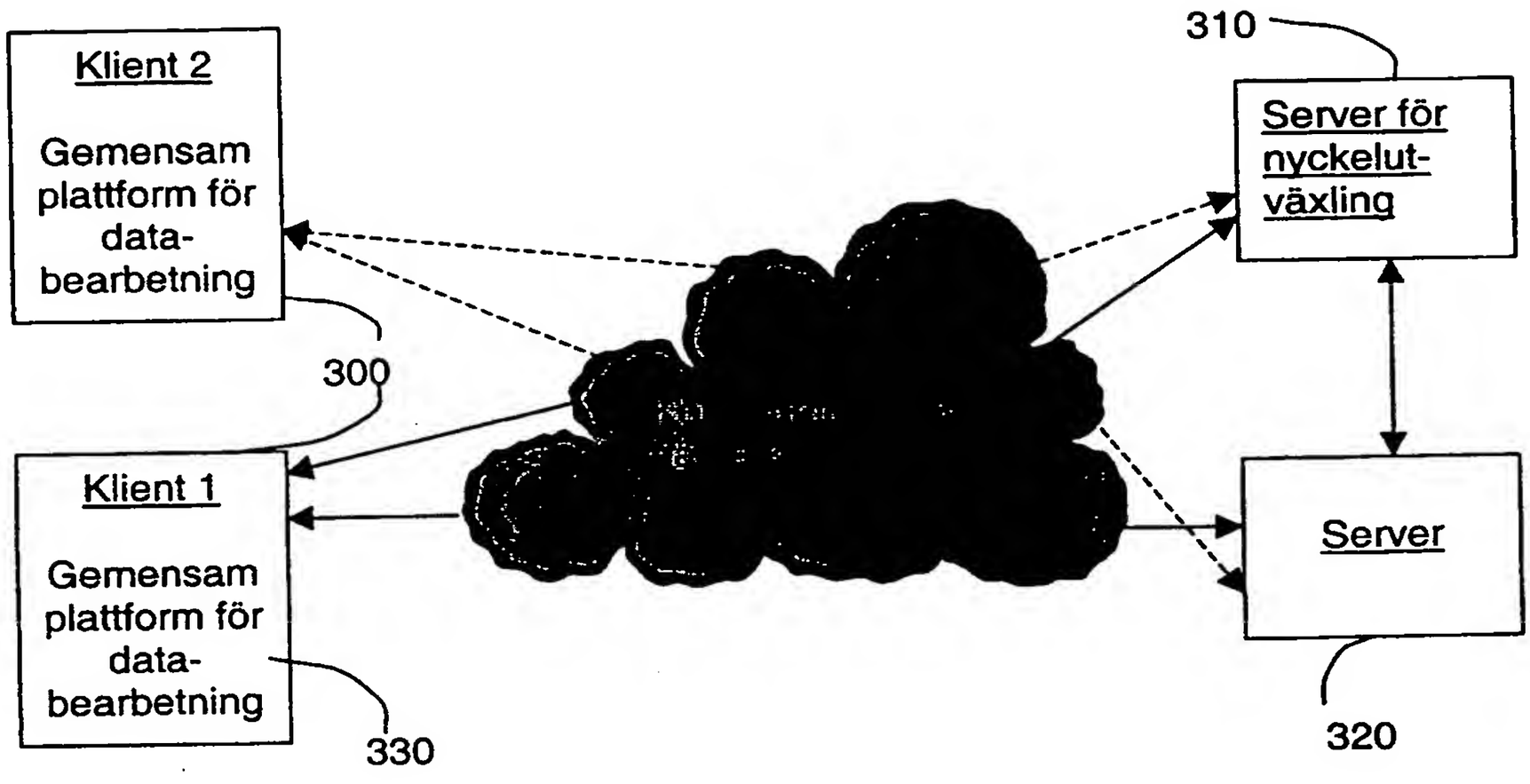
10. Metoden enligt något av kraven 6-9 **kännetecknad av** att nämnda server är en server för utväxling av nycklar försedd med organ för att kunna tillhandahålla en huvudnyckel gällande en viss grupp för att skydda kommunikationen för ett flertal tjänster.


110
Klient
Gemensam plattform för data-bearbetning
140
130
120
Server

Figur 1


SÖK EFTER EN TJÄNST
LADDA NED EN PROXY
VERIFIERA DEN NEDLADDADE PROXYNS SIGNATUR
EXEKVERA DEN NEDLADDADE PROXYN OM VERFIERINGEN UTFALLER TILL BELÅTENHET
PROXYN UTFÖR UTVÄXLING AV ÄKTA NYCKLAR PÅ ETT SÄKERT SÄTT
EN SÄKER KOMMUNIKATIONSKANAL UPPRÄTTAS

Figur 2.


Klient 2
Gemensam plattform för data-bearbetning
300
Klient 1
Gemensam plattform för data-bearbetning
330
310
Server för nyckelut-växling
Server
320

Figur 3